CAC Execution Plan

Executive Summary

The Department of Defense (DoD) has initiated an aggressive plan to implement smart card technology throughout the Department. This implementation will include all active duty military personnel, the Selected Reserve, DoD civilian employees and eligible contractor personnel. The Department's smart card, known as the Common Access Card (CAC), will become (1) the standard identification card, (2) the means to gain physical access to buildings and controlled spaces, and (3) the means to gain access to the Department's computer networks and systems. The Department's smart card platform will include multiple commercially derived technologies (i.e., an embedded integrated circuit chip, bar codes, magnetic stripe, and a digital photograph of the cardholder) hosted on a single plastic card.

This CAC Execution Plan is in response to the Deputy Secretary of Defense (DEPSECDEF) memorandum of November 10, 1999. In that memorandum, the DEPSECDEF directed that the Department's initial implementation of smart card technology be effected as a Department-wide common access card and required that an Execution Plan be developed for the CAC. This Plan covers a management concept of operations, a methodology for requirements planning, the use of Functional Community Panels, and an overview of configuration management. A Milestone Chart with key events for CAC implementation is also included.

In order to deploy a Department-wide CAC beginning in October 2000, several decisions must be made in the near-term. These decisions include completing the requirements definition; defining CAC platform specifications; and finalizing a strategy for procuring necessary smart card hardware, firmware, and software. Other key milestones within the next six months cover the development of government-wide interoperability specifications by the General Services Administration (GSA) and industry partners (June 2000), beta testing the CAC (August 2000), and finalizing the CAC configuration for the fielded version (September-December 2000).

The Department has made significant strides toward CAC execution. With the establishment of the Smart Card Senior Coordinating Group (SCSCG) and the Smart Card Configuration Management Control Board (SCCMCB), the Department has leadership and decision making groups in place to manage and ensure effective implementation. Membership for both the SCSCG and SCCMCB is comprised of senior representatives and decision-makers from the Office of the Secretary of Defense (OSD), the Joint Staff, Military Services, and Defense Agencies (collectively known as DoD Components). Representatives from key organizations, such as the Offices of the Principal Staff Assistants

(PSAs) within the Office of the Secretary of Defense (OSD), including the DoD Chief Information Officer (CIO), the Military Services, including the Department of the Navy CIO, the Defense Manpower Data Center, the Access Card Office, the Public Key Infrastructure (PKI) Program Management Office, and Service smart card offices are participating in CAC planning and implementation issues on a daily basis.

The DoD organization, requirements, resources, and schedule will help to ensure that the CAC is executed on time and is consistent with stated requirements. Execution, as referred to in this plan, refers to the initial fielding and supply of CACs to the identified target population. The Execution Plan lays the groundwork for lifecycle management of the CAC. Components may require additional time to plan, develop requirements, and budget for CAC use. With the implementation of the CAC and its management infrastructure, the Department is essentially implementing a tool for all of its Components to use in re-engineering their respective business processes. This tool will have a minimum *capability* of identification, physical access, and logical access. In this sense, *capability* does not imply authorization or ability. Specific access to physical areas and DoD computer systems will be granted by the Components and/or their designated representatives.

Significant changes to existing policies and/or implementation of new policies governing functional areas of the CAC, such as identification, PKI, and physical access may have to be made at the DoD and Component level. Critical near-term decision milestones have been addressed in order to finalize the CAC platform specifications, which, in turn, will decide the smart card type, chip allocations, and card topology. The schedule to begin implementation by October 2000 is aggressive but can be executed with continued cooperation from the key organizations within the DoD Components. The regular meetings of the SCSCG and the SCCMCB, as well as the Functional Community Panels, are essential to ensure top-down management attention and CAC success. Successful execution of the CAC will be a significant part of the Department's continued commitment to innovation using business process re-engineering (BPR) and technology to improve business practices and information assurance.

Table of Contents

1. Introduction

Converging events--such as Vice President Gore's National Partnership for Reinventing Government, the Defense Reform Initiative, the restructuring and consolidation of Department of Defense (herein referred to as DoD or the Department) and Service infrastructures, and a maturing information technology (IT) base--have culminated in the need for new solutions to improve the way business is conducted. The Revolution of Business Affairs, under the Defense Reform Initiative, means "adopting and adapting the best business practices of the private sector to the business of defense." Reforms in electronic business (to include paperless contracting, wide-area workflow, and other procurement and finance applications), travel re-engineering, and expanded use of the government-wide commercial purchase card program coupled with information assurance for data and user authentication have presented new opportunities to use smart card technology as an enabling tool for business process improvement. Smart card technology also can offer an additional layer of electronic security and information assurance (i.e. authentication, confidentiality, non-repudiation, information integrity, confidentiality, and access control). This is particularly important as the Department continues to expand the scope of its electronic information enterprises with efforts such as the Global Information Grid (GIG) and the Navy and Marine Corps Intranet (NMCI).

The purpose of this Common Access Card (CAC) Execution Plan is to document the requirements planning methodology, concept of operations, and schedule for deploying the CAC Department-wide. This Plan also addresses the use of cross-Component Functional Community Panels to ensure communication and the pooling of expertise in the development of Department-wide applications for the CAC platform. Further, the Plan identifies CAC program risks and how these risks will be minimized. The Plan goes on to describe a CAC configuration management process; a full, comprehensive Configuration Management Plan is being developed separately.

1.1 Scope

This Execution Plan focuses on actions required for the initial rollout of the CAC in December 2000 (first quarter FY 2001), to be completed by September 2002. However, continuing efforts will be required to incorporate emerging requirements for smart cards in the Department (e.g. PKI Class 4). This will be accomplished in two ways:

- Overarching strategic planning for smart card technology in the Department

- Configuration management process for incorporating new capabilities and/or functions

The DoD smart card technology strategy must be consistent and complementary to Department planning documents such as Joint Vision 2010, Defense Reform Initiatives, Information Management (IM) Strategic Plan, and the DoD Electronic Business/Electronic Commerce (EB/EC) Strategic Plan. The DoD smart card technology strategy must comply with statutory requirements such as the Information Technology Management Reform Act (Clinger-Cohen Act).

Both the IM Strategic Plan and EB/EC Strategic Plan contain initiatives and references to smart card technology made prior to the November 10, 1999, DEPSECDEF decision to adopt smart card technology in the form of the CAC. The documented strategy for smart card use in the Department is to enhance mission support functions such as logistics, finance, health, and personnel. While mission support functions are still applicable, the strategy must be revised to encompass the functions stated in the DEPSECDEF memorandum: logical access, physical access, and identification.

In an effort to pursue a strategic planning effort for smart card technology across the Department, the SCSCG has tasked the DoD ACO to develop a strategy for smart card implementation within the Department. This strategy will leverage to the fullest extent possible the existing strategic planning efforts such as the IM Strategic Plan and EB/EC Strategic Plan. In lieu of creating an independent planning process and separate strategic plan, existing strategic planning efforts will be evaluated and updated in the next planning cycle to reflect the direction of smart card technology within the Department. The DoD ACO will be the SCSCG's agent as an active participant in the DoD CIO/OASD(C3I) strategic planning process for information technology systems.

In addition to strategic planning, the configuration management process developed for the CAC will identify operating and management parameters for the CAC post-issuance (i.e., version 2.0 and later). Section 7.0 of this plan provides an overview of CAC configuration management, while a separate Configuration Management Plan details the CM process.

1.2 Authority

Under the Defense Reform Initiative, the Department is committed to innovation through the reformation of business processes and exploitation of technology to achieve efficiencies and improve readiness. Consistent with the Clinger-Cohen Act of 1996 (Divisions D and E of Public Law 104-106) and the Fiscal Year 2000 Defense Authorization Act (Public Law 106-65) of October 1999, the DoD CIO is

assigned overall responsibility for the development of the Department's Smart Card Policy and Oversight.

The Fiscal Year 2000 Defense Authorization Act (Public Law 106-65) designated the Department of the Navy as the lead Service for the development and implementation of DoD smart card technology. This included the establishment of smart card project offices by the Departments of the Army and Air Force, along with cooperation of those newly established offices within the Department of the Navy. The primary purpose of these offices is to develop implementation plans exploiting the capability of smart card technology as a means for enhancing readiness and improving business processes across the DoD Components (i.e., the Office of the Secretary of Defense (OSD), the Joint Staff and the Combatant Commands, the Military Departments, the Defense Agencies, and the DoD Field Activities).

Public Law 106-65 mandated the establishment of the SCSCG to develop and implement Department-wide interoperability standards for use of smart card technology and to develop and implement a plan to exploit smart card technology as a means for enhancing readiness and improving business processes. The law mandated that the SCSCG be chaired by a representative designated by the Secretary of the Navy and include senior representatives from each of the Military Services as well as other officials deemed appropriate by the Secretary of Defense.

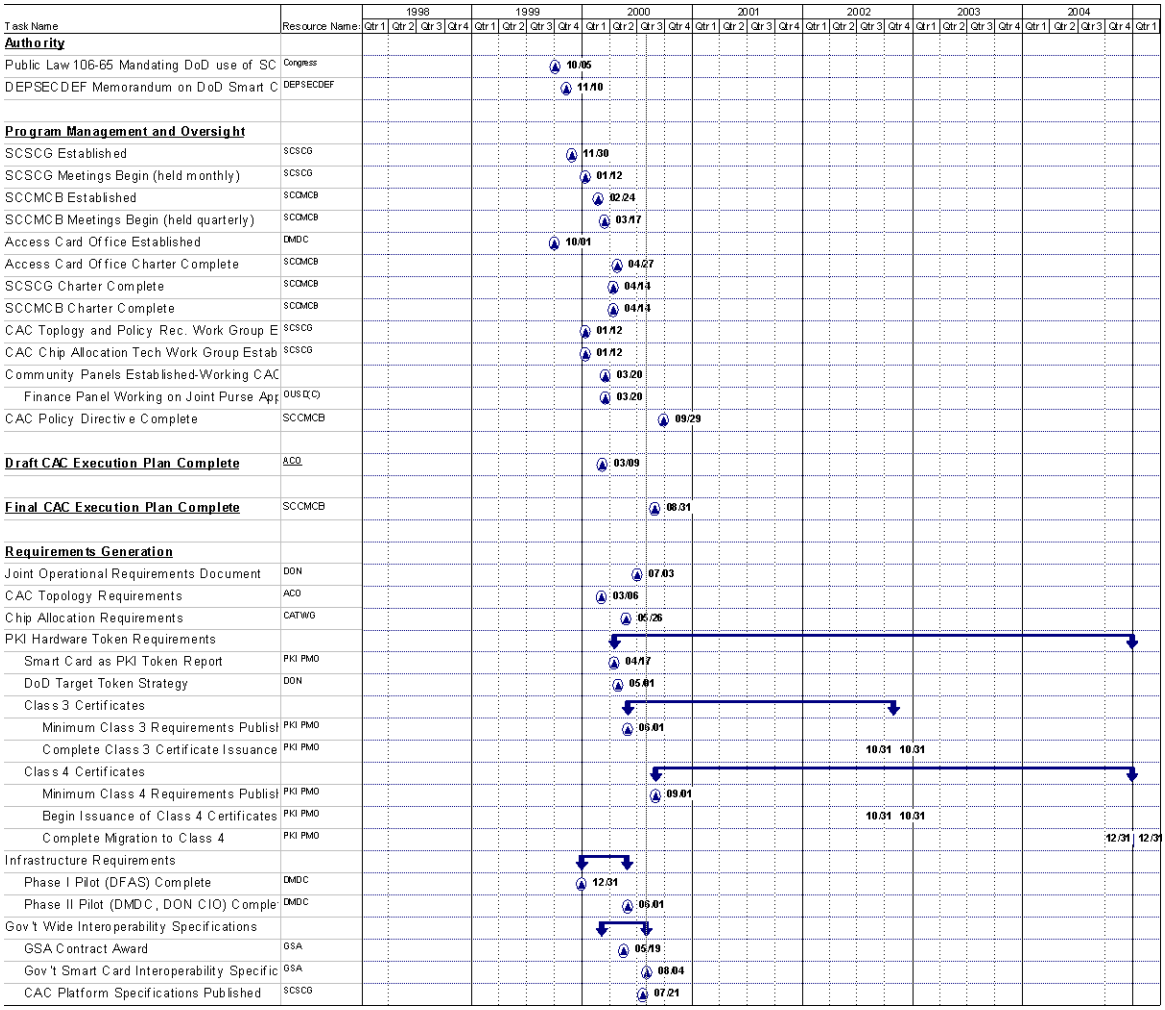
A Deputy Secretary of Defense (DEPSECDEF) memorandum, issued on November 10, 1999, directed the Department initially to implement smart card technology as a Department-wide CAC. This memorandum further defined the target population for the CAC as active duty military personnel, the Selected Reserve, DoD civilian employees, and eligible contractor personnel. The Selected Reserve includes Selected Reserve Units (i.e. Drilling Unit Reservists and Full-time Reserve Unit Support Personnel), Trained Individuals (i.e. Individual Mobilization Augmentees (IMAs)), and Training Pipeline personnel. . DoD civilian employees, as defined in Title 5, United States Code, section 2105, are individuals appointed to positions by designated officials. Eligible contractor personnel generally are employees of firms or individuals under contract or subcontract to a DoD Component, designated as providing services or support to a Component that requires physical and/or logical access to the facilities and/or systems of the Department. This initial CAC target population does not include military or civilian retirees, family members, members of the Individual Ready Reserve (IRR), Inactive National Guard (ING), Standby Reserve, Retired Reserve, or contractors working outside of DoD facilities and networks. The CAC shall be the standard identification card for this population and provide physical access to buildings and controlled spaces, along with access to the Department’s computer networks and systems.

In addition to creating the congressionally mandated SCSCG, the DEPSECDEF memorandum established the SCCMCB, which replaced the former Smart Card Senior Steering Group. The Department also established an Access Card Office (ACO), which succeeded the former Smart Card Technology Office (SCTO), and remains an element of the Defense Manpower Data Center (DMDC). Details regarding the roles and responsibilities of these groups are further described in the following sections.

2. Execution Timeline

The primary focus of DoD representatives involved in the development and deployment of the CAC should be an interoperable and integrated solution, which can support future uses by the Department and its Components. Much like the use of computers within the Department, it is expected that smart card technology will be an evolving platform that will require additional follow-on efforts, such as lifecycle management and technology refreshment, not addressed by this timeline. The timeline for developing and fielding the CAC is aggressive and must be supported by a well-coordinated management infrastructure. This timeline supports CAC issuance to the target population via normal attrition during fiscal year (FY) 2001 and to the remainder of this population during FY 2002. The specific approach to conduct this issuance is left to the Components. The major milestones for Calendar Years 2000 and 2001 are depicted in the CAC Milestone Chart (Figure 1).

CAC Milestone Chart -- Figure 1



CAC Milestone Chart -- Figure 1 (cont'd)

Task Name	Resource Name	1998 Qtr 1	1998 Qtr 2	1998 Qtr 3	1998 Qtr 4	1999 Qtr 1	1999 Qtr 2	1999 Qtr 3	1999 Qtr 4	2000 Qtr 1	2000 Qtr 2	2000 Qtr 3	2000 Qtr 4	2001 Qtr 1	2001 Qtr 2	2001 Qtr 3	2001 Qtr 4	2002 Qtr 1	2002 Qtr 2	2002 Qtr 3	2002 Qtr 4	2003 Qtr 1	2003 Qtr 2	2003 Qtr 3	2003 Qtr 4	2004 Qtr 1	2004 Qtr 2	2004 Qtr 3	2004 Qtr 4	Qtr 1
CAC Evaluation Criteria																														
Business Case Methodology Developed and	ACO		04/07																											
CAC Evaluation Criteria Established	ACO											07/03																		
CAC Business Case Analysis Complete for I	ACO															09/03														
Functional Requirements																														
Functional Requirements defined in DEPSEC	DEPSECDEF								11/10																					
Additional Dept-wide Applications Approved f	SCCMCB										05/31																			
Community Panel Guidance (CAC Execution	ACO											08/31																		
Finance Community Panel Recommendation	OUSD(C)											08/31																		
Uniformed Service ID Changes	OUSD(P&R)										04/05																			
Baseline Solution and Manage Configurat																														
Finalize Agreement of CAC Data Elements	SCSCG											07/05																		
Assign Action Components for CAC Applicati	SCCMCB											08/01																		
Draft Configuration Management Plan to SCS	ACO										05/22																			
Draft Configuration Management Plan to SCC	SCSCG											08/16																		
Configuration Management Plan Complete	ACO											08/31																		
Issue Application Development Guidance to C	DMDC											06/30																		
Beta Testing and Fielding																														
Fielding Plan Complete (Issuance HW)	DEERS/RAPIDS PC											08/03																		
Finalize CAC configuration for Beta Tests	ACO											07/05																		
Stand up Beta Sites	DMDC												10/03																	
Beta Testing for CAC Complete	ACO													12/15																
Finalize CAC configuration for Fielded Versio	ACO												09/29																	
PKI Integrated Work Station Security Assess	DMDC / NSA													11/15																
Broad Communication																														
Smart Card Communications Plan Complete	ACO											07/14																		
ACO Web Site Initial Version Complete	ACO											08/02																		
CAC Implementation																														
Initial Operation Capability - Rollout														12/01																

3. Management Concept of Operations

3.1 Purpose and Scope

The purpose of this section is to identify a management concept for the operation of the SCSCG and SCCMCB and their respective interactions with the DoD Components (to include the Functional Community Panels). In addition, this concept of operations defines the flow of information and communications among the Department's CIO, the SCCMCB and SCSCG, the Department of the Navy (as the designated chair of the SCSCG), the DoD Components, the ACO, and the Public Key Infrastructure (PKI) Program Management Office (PMO).

3.2 Mission Statement of the Department of Defense Smart Card Program

The smart card will provide the Department with a multi-application technology solution that enables positive identification of personnel seeking access to DoD services, facilities, computer networks, and systems, and enables the efficient re-engineering of DoD business processes.

3.3 Vision Statement of the Department of Defense Smart Card Program

By 2005, the Department will have a single medium in place that provides its personnel an easy (portable) identification capability for access to and transfer of personal information among DoD services, facilities, computer networks, and systems while providing the Department with information assurance and business process efficiency.

3.4 Conceptual Framework

It is important to separate centralized and decentralized functions with regard to management of the CAC. The representatives involved with CAC implementation and oversight at the Department level should limit their responsibility to centralized functions. Figure 2 delineates centralized and decentralized functions.

CAC Centralized and Decentralized Functions -- Figure 2

CENTRALIZED	DECENTRALIZED
Program Governance, e.g.: ? ? Policy regarding workstation operations ? ? Certificate Practice Statement (CPS) ? ? Training documentation for workstation operators ? ? Hardware specification guidance	Component-specific applications
Mandated Applications, e.g.: ? ? PKI ? ? Building Access ? ? Logical Access ? ? ID Cards	Physical access authorization enablement (Granting of Privileges Regarding Logical Access)
Issuance Policy	System access authorization enablement (Granting of Privileges Regarding Logical Access)
DEERS/RAPIDS Hardware and Software for initial mandated CAC applications issuance and support	Management of DEERS/RAPIDS/LRA workstation operations
Department-wide Applications, e.g.: ? ? Manifesting ? ? e-Purse ? ? Food Service	Applications Hardware
Core Data Elements and Applications on the ICC	BPR
ICC Memory Allocation for Components	Execution of CAC Functions (post fielding)

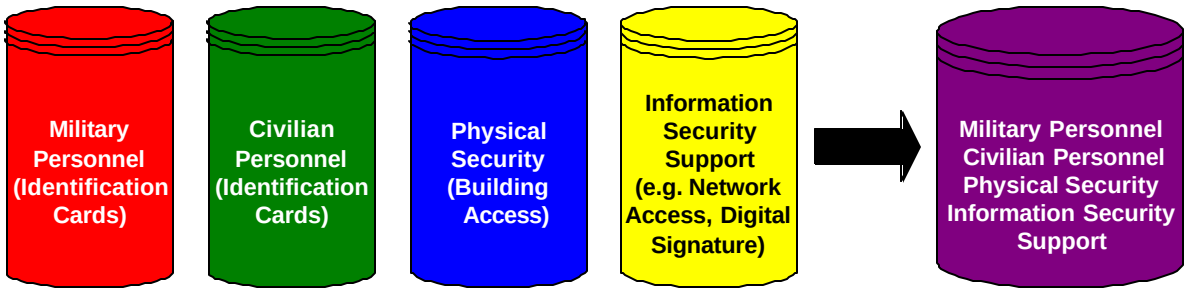
One other important aspect for management consideration is the transition from multiple, single-function infrastructures towards a single, multi-function infrastructure (using the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-time Automated Personnel Identification System (RAPIDS) infrastructure) in order to issue CACs and maintain the associated CAC database. As indicated in the Department of Navy (DON) Smart Card Office (SCO) Re-engineering Phase I Business Plan for Personnel Support Detachment Pearl Harbor (June 1999), this transition will result in improvements to current business processes by consolidating issuance functions while

leveraging existing infrastructure. Due to the additional requirements and needs of specific communities, such as Intelligence, it is recognized that not all will make this transition, but the majority of the target population will. The CAC itself will be capable of carrying Sensitive But Unclassified (SBU) information. The capability for the CAC to provide individuals access to higher security level physical areas and logical domains can be correlated to the PKI class level, but is ultimately the decision of the Component or designated authority.

With the incorporation of PKI onto the CAC, a number of issues arise related to card management and lifecycle. These issues are being addressed by the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (OASD)(C3I)) and closely coordinated via the ACO. The OASD(C3I) has established work groups, such as the DoD PKI Technical Working Group, the DoD PKI Business Working Group, and the DoD Certificate Policy Management Working Group to address those issues related to the DoD PKI. These groups and those established by the SCSCG should coordinate their efforts to avoid overlaps in addressing issues within their respective scope and expertise. Several references, such as the DoD PKI Implementation Plan, DoD Public Key Infrastructure Roadmap, DoD PKI Policy Planning Document, DoD Certificate Policies, and Certificate Practice Statements, have been or are being developed to provide guidance on these issues.

The policy for Uniformed Services Identification Cards is, and will continue to be, a centralized function. The issuance of Uniformed Services identification and civilian identification, and the grant of access and privileges to secure spaces and computer systems are Component responsibilities. The CAC will be issued with the *fundamental* *capability* (but not the *permission*) to access DoD controlled areas and networks. Permission separately will be controlled by individual Components and/or their designated representatives for physical and logical access. The transition management illustration below displays how functions, which,at present, separately are executed, now will be carried out using a single infrastructure. An illustration of the infrastructure transition management is depicted in Figure 3.

CAC Transition Management -- Figure 3

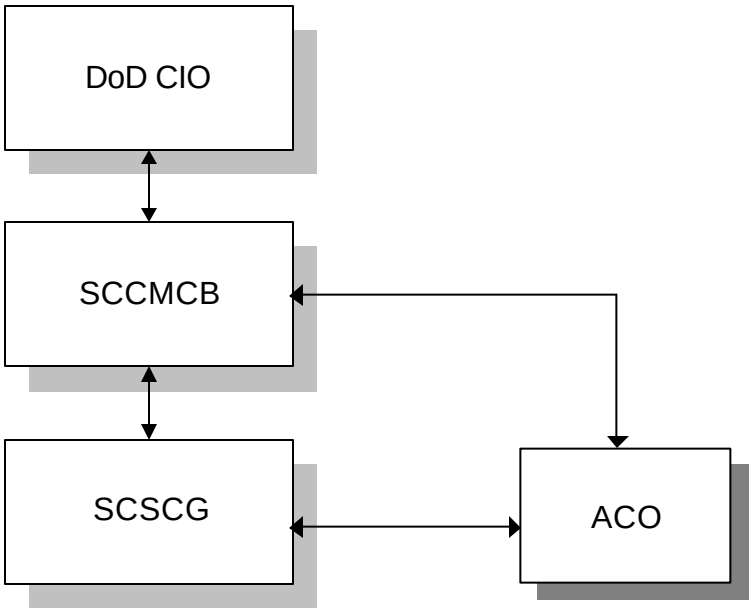


3.5 Functional Concept

3.5.1 Management

The three primary organizations involved at the Department level to support the CAC are the SCCMCB, SCSCG, and the ACO. The management roles and responsibilities of these three organizations are addressed in the next section. The organizational structure for these entities is depicted in Figure 4.

SCCMCB, SCSCG, and ACO Organizational Structure -- Figure 4



3.5.2 Management Roles and Responsibilities

3.5.2.1 SCCMCB

The SCCMCB's primary responsibility is to assure the integration of cross-functional requirements to determine summary-level chip storage allocations, to include those for Component-specific use of the CAC. The SCCMCB oversees the operation of the SCSCG.

The SCCMCB explicitly performs the following functions:

✍✍Assure the integration of cross-functional requirements

- Act upon recommendations made by the SCSCG with respect to DoD-wide implementation of Component-specific, CAC configuration, and PKI implementation

- Approve reports to the Congress on smart cards for release by the DoD CIO or higher authority, as appropriate

- Assure broad communication and cross-functional integration of smart card initiatives

- Oversee the operation of the SCSCG

- Guide the SCSCG to develop and implement Department-wide interoperability standards for use of smart card technology

- Guide the SCSCG to develop and implement a plan to exploit smart card technology as a means for enhancing readiness and improving business processes

- Provide strategic direction, planning, and guidance to the SCSCG and DoD Components on the development and implementation of smart card technologies within the Department

- Establish and ensure adherence to the Department's smart card vision

- Provide for the integration of smart card requirements into the DoD Information Assurance Program[1]

3.5.2.2 SCSCG

The SCSCG's primary responsibility is to develop and oversee Department-wide interoperability standards for use of smart card technology and a plan to exploit smart card technology as a means for enhancing readiness and improving business processes. This group integrates smart card requirements in coordination with the DoD Components and the PKI PMO, making all recommendations to the Department's CIO through the SCCMCB.

The SCSCG explicitly performs the following functions:

- Develop and oversee the implementation of Department-wide interoperability standards for use of smart card technology

[1] Smart Card Configuration Management Control Board Charter dated April 14, 2000

- Develop and implement a plan to exploit smart card technology continually as a means for enhancing readiness and improving business processes

- Implement guidance from the DoD CIO and SCCMCB

- Make recommendations to SCCMCB with respect to DoD-wide implementation of Component-specific applications, CAC configuration, and PKI implementation

- Coordinate smart card applications in conjunction with the senior functional and operational managers who are responsible for those missions and functions that are to be supported by the CAC

- Prepare reports to the Congress on smart cards, through the DoD CIO and Secretary of Defense, as required

- Provide strategic direction and guidance to develop and implement the CAC and smart card technologies within the Department

- Ensure adherence to the Department's smart card vision

- Integrate the smart card requirements in coordination with the DoD Components and the PKI PMO, and make recommendations to the SCCMCB

- Serve as the DoD-wide advocate for smart card issues[2]

3.5.2.3 ACO

The ACO provides operational, technical, program and policy support, and associated information management to the Department's CIO, SCSCG and the SCCMCB. The ACO is an element of DMDC, and is under the operational control of the Department's CIO and under the policy direction and oversight of the SCCMCB and the SCSCG.

The ACO explicitly performs the following functions:

- Provide support to the Department's CIO, SCCMCB, SCSCG, Principal Staff Assistants, Joint Staff, and other DoD Components in the execution of smart card policies and programs including acting as a central clearinghouse for functional and policy requirements to assure appropriate coordination,

[2] Smart Card Senior Coordinating Group charter dated April 14, 2000

integration, and implementation

- Administer assigned Department-wide smart card programs, in concert with the Department's CIO

- Serve as Executive Secretary to the SCSCG and SCCMCB

- At the direction of the SCCMCB and the SCSCG, conduct studies and analyses, prepare technical and administrative reports, decision papers, white papers, or other documentation

- Develop, under the Department's Standards Program, proposed Department-wide interoperability standards for use of smart card technology for review and approval of the SCSCG and the SCCMCB[3]

3.5.3 Composition

3.5.3.1 SCCMCB

The SCCMCB is a senior level group that includes flag or Senior Executive Service (SES) level representatives from the organizations below and other organizations by invitation. The Chair of the SCCMCB is a designated representative of the DoD CIO. The SCCMCB is specifically composed of representatives from the following organizations:

- Office of the Under Secretary of Defense (OUSD)(Policy)
- OUSD (Acquisition, Technology and Logistics)
- OUSD (Comptroller)
- OUSD (Personnel and Readiness (P&R), with representation as denoted in Appendix C
- Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) (Chair)
- Director, Program Analysis and Evaluation
- Joint Staff
- Department of the Army
- Department of the Navy
- Department of the Air Force
- United States Navy
- United States Marine Corps
- Intelligence Community (IC) CIO
- PKI PMO

[3] Access Card Office Charter dated April 27, 2000

?? ACO (Executive Secretary)
?? Advisors to the Control Board are from the following offices:
  ?? National Security Agency (NSA)
  ?? Defense Information Systems Agency (DISA)
  ?? General Counsel of the DoD (GC, DoD)
  ?? Program Manager-Defense Travel System

3.5.3.2 SCSCG

This group is chaired by an official (Flag/SES) appointed by the Secretary of the Navy. The SCSCG specifically is composed of representatives from the following organizations:

?? OUSD (Policy)
?? OUSD (Acquisition, Technology and Logistics)
?? OUSD (Comptroller)
?? OUSD (P&R), with representation as denoted in Appendix C
?? OASD(C3I)/DoD CIO
?? Program Analysis and Evaluation
?? Joint Staff *
?? Department of the Army
?? Department of the Navy (Chair)
?? Department of the Air Force
?? United States Navy
?? United States Marine Corps
?? DMDC
?? Defense Logistics Agency (DLA)
?? DISA
?? NSA
?? Defense Finance and Accounting Service (DFAS)
?? Other Selected Defense Agencies **
?? PKI PMO
?? IC CIO
?? GC, DoD
?? Other organizations (by invitation)
?? ACO (Executive Secretary)

* It is expected that the Joint Staff will coordinate appropriate Commander-In-Chief (CINC) representation.

** Selected Defense Agencies are expected to include those that currently are involved or interested in the use of smart card technology.

3.6 Oversight and Coordination

All designated representatives who are members of the SCCMCB and SCSCG are expected to coordinate smart card-related issues with their respective organizations to the maximum extent practicable. While there may not be full agreement on all issues, members of these bodies should strive to attain consensus in the interest of meeting the aggressive timeline for CAC implementation.

Work groups may be established by the SCSCG to provide support as necessary. The SCSCG should leverage the capabilities of existing DoD work groups to the maximum extent possible. Direction and expertise for the groups should be clear and concise. Two work groups, one to address CAC topology and policy and the other to address CAC chip allocation, have been established by the SCSCG.

Department-wide CAC applications can be proposed by three means:

(1) Existing smart card pilots supported within the Department. This is a one-time occurrence involving backward compatibility. Existing Department smart card application pilots (e.g. Joint Warrior Readiness, Food Service, and Manifesting/Tracking) will undergo a decision process for continued support by the CAC platform. A Functional Community Panel will need to be established for lifecycle maintenance of the selected application(s), including initial migration to the CAC.

(2) Functional Community Panels. These may be established by functional sponsors, such as the PSAs to develop requirements for specific Department-wide CAC applications. The OSD PSAs include the Under Secretaries of Defense (USD), the Director of Defense Research and Engineering (DDR&E), the Assistant Secretaries of Defense (ASDs), the Director of Operational Test and Evaluation (DOT&E), the General Counsel of the Department of Defense (GC,DoD), the Inspector General of the Department of Defense (IG,DoD), the Assistants to the Secretary of Defense (ATSDs), and the OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense. Depending on PSA preference, Functional Community Panels may be standing or ad-hoc (i.e., established and disestablished as needed). Functional Community Panel chairpersons are expected to keep the SCSCG informed of key decisions and requirements, particularly as they apply to CAC architecture. One example of a Functional Community Panel is the Finance Functional Community Panel established by the USD (Comptroller), which currently is investigating the feasibility of an electronic purse application on

the CAC.

(3) Component recommendation. Components will recommend applications for Department-wide development via the SCSCG. The SCSCG then will work with the cognizant PSA to establish a Functional Community Panel to coordinate application requirements.

Components do not need Department-level approval for development and implementation of Component-specific applications for the CAC. From a configuration management perspective, Component-specific applications will need to be coordinated at the Department level to test their impact on the CAC and to share application information across the Department. This will leverage previous application development and prevent duplicative efforts by other Components. These issues are addressed in more detail in the CAC Configuration Management Plan.

Timely and extensive communication is necessary to ensure successful DoD-wide implementation of the CAC. In order to achieve this end, the majority of communications and staffing will take place electronically, but the SCSCG and SCCMCB should allow sufficient time to properly staff reports and plans, ensure all issues are raised and addressed, and organizations are allowed time to review updated reports and plans with resolution of comments. At least initially, meetings of the SCSCG will take place on a monthly basis, while meetings of the SCCMCB will be quarterly, or otherwise as required.

The SCSCG and the SCCMCB shall ensure that sufficient time is provided for staff reports among all interested Components. All coordination parties shall expedite staffing of CAC-related reports and information. Appropriate Office of General Counsel (OGC) review also shall be given to all documents generated and forwarded by the SCCMCB and SCSCG. The OGC specifically should be involved in matters with legal and privacy implications, such as use of biometrics for identification or the use of digital or electronic signature in lieu of a hand written signature.

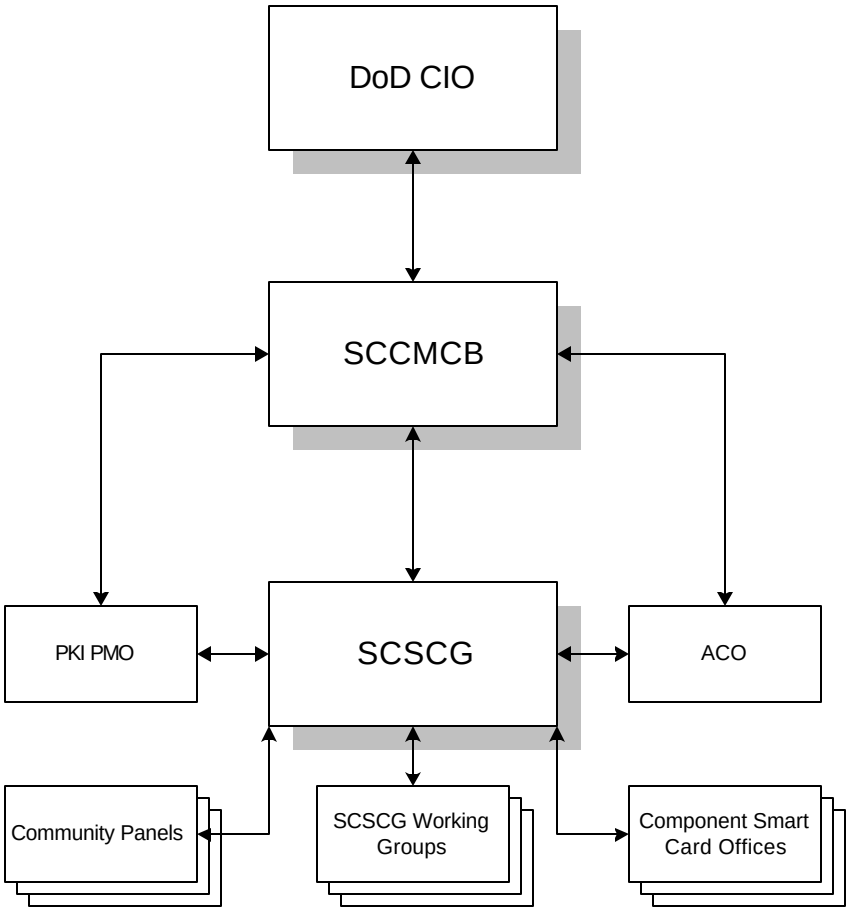
Successful implementation of the CAC requires close coordination with the PKI PMO to merge requirements and timelines such that the CAC may meet the requirement for primary user authentication. Two strong reasons for close involvement by the PKI PMO in development of the CAC are to (1) assure that PKI requirements are satisfied and (2) verify that non-PKI applications do not adversely affect the PKI tokens placed on the imbedded chip.

The management organization will also engage the physical security and Information assurance communities to enable the CAC as a tool, respectively for physical and logical access.

The smart card, as an emerging technology, may necessitate the establishment of technical standards by the Department. The Department intends to use and leverage existing industry smart card standards to the maximum extent practicable and support the government-wide interoperability standards with the CAC. The Department is participating in the Government-wide Smart Card Interoperability Standards development along with industry smart card-related standards to maximize the interoperability of the CAC and enable the support of open specifications and standards where possible. This effort will be coordinated through the Department's Standards Coordinating Committee (SCC), which is chaired by a DISA representative. The CAC will also comply with the Joint Technical Architecture (JTA) standards as documented.

Figure 5 displays the coordination and information flow necessary effectively to manage and implement the CAC and smart card technology.

CAC Coordination and Information Flow -- Figure 5



3.7 Functional Community Panels

3.7.1 Introduction

As presented in the November 1999 DEPSECDEF memorandum, Functional Community Panels will be employed to ensure broad communication and integration among and between functional areas within the Department. Within the Department, Functional Community Panels traditionally have been used to facilitate the coordination of policy where the policy concerns more than one DoD Component and, possibly, other federal agencies. Functional Community Panels regularly are used as recommending bodies on similar issues affecting a functional area. At their inception, the smart card programs in the Department have used Functional Community Panels or functional area work groups to support the generation of requirements from process owners and end-users. The use of Department-wide smart card applications for pilot programs and demonstrations necessitated the need to bring all affected Components together in a forum to generate requirements, leverage existing infrastructure, and disclose lessons learned.

3.7.2 Functional Community Panel Purpose

To ensure that the Department's objectives of broad communication and functional integration are met, the Functional Community Panels have a two-fold purpose:

- Evaluate the need for smart card technology within a functional area using such factors as cost savings, investment, risk, mission enhancement, and impact to quality of life
- Through the cognizant PSA, provide recommendations as to whether an existing smart card application makes business sense, supports policy and operational requirements, and is technically feasible for Department-wide use (on the CAC).

3.7.3 Functional Community Panel Operations

Intentionally, there has been little guidance or direction on how Functional Community Panels would operate. The OSD PSAs have the ultimate responsibility and authority to create Functional Community Panels for the purposes mentioned above. The Functional Community Panels may be designated as ad-hoc and focused on explicit tasking or may be formed on a standing basis to evaluate a series of issues relating to smart card technology. The Functional Community Panel members, with PSA approval, generally formulate their own charter, including operating standards, organizational

structure, membership, and responsibilities. Upon identifying that a need exists for smart card technology within a functional area, the Functional Community Panel may conduct the feasibility analysis, develop requirements using the requirements planning methodology outlined in section 4, and oversee development, execution, and maintenance of the application. There are no provisions for the ACO to manage Department-wide application development. As a result, the Functional Community Panels, with the approval of respective PSAs, must designate an Action Component to manage approved Department-wide application development and implementation.

Some critical success factors common throughout all Functional Community Panels include:

- Top-down agreement of the Functional Community Panel and its purpose
- Well defined roles and responsibilities that support the Community
- Consistent representation across the DoD Components
- Membership that is commensurate with the Functional Community Panel's objective (e.g., senior personnel who possess working knowledge of the business process and understand impacts to policy DoD-wide with the ability to formulate decisions and recommendations)
- The latitude to change the Functional Community Panel charter to accommodate new objectives
- The ability to recommend the implementation of a smart card application based upon business-based criteria and requirements.

3.7.4 Finance Community Panel

Presently, one of the Functional Community Panels, known as the Finance Community Panel, exists to generate requirements for financial smart card application(s). Other Functional Community Panels are expected to form once the core CAC requirements for logical access, physical access and identification/authentication are finalized.

The Finance Community Panel was formed following creation of the previous SCTO (then referred to as the Finance Functional Work Group). The Principal Deputy USD (Comptroller) signed a memorandum requesting that the Director of DFAS host and perform Executive Secretary responsibilities for this Functional Community Panel. Functional Community Panel membership includes representatives from the OUSD (Comptroller), DFAS, the Offices of the Assistant Secretaries of the Military Departments (Financial Management and Comptroller), and the Department of the Treasury (advisory). Other organizations that have participated with this Functional Community Panel include the DON SCO (an established office for Smart Card programs), and the

Naval Supply Systems Command (NAVSUP), which manages the ATM-at-Sea Program.

The primary mission of the Finance Community Panel is to evaluate opportunities for and benefits of using smart cards to facilitate financial applications (e.g., electronic purse function, stored value, debit/credit function). Several pilot programs and demonstrations (nine to date) are currently underway or completed with published results. The focus of this Functional Community Panel prior to the November 1999 DEPSECDEF memorandum was the management and evaluation of pilot programs for application feasibility based upon cost savings, mission enhancement, and quality of life improvements for DoD personnel. To support the requirements of the CAC, this Functional Community Panel currently is determining the chip space allocation for a financial application, the use and impact of commercial bank/network logos printed on the card, and financial systems security. The formulation of a Functional Community Panel recommendation as to whether a viable Department-wide financial application should reside on the CAC or be separate on a stand-alone card has been a primary focus. This recommendation will be through the USD(C) to the ACO and the SCSCG.

3.7.5 Joint Uniformed Services Personnel Advisory Committee

An example of a Functional Community Panel established to recommend policy for the execution of the Uniformed Services Identification Card is the Joint Uniformed Services Personnel Advisory Committee (JUSPAC). The JUSPAC consists of members from each of the Uniformed Services (Army, Navy, Air Force, Marine Corps, Coast Guard, Public Health Service, and National Oceanic and Atmospheric Administration, and associated Reserve Component organizations). Representatives from OUSD(P&R), DEERS/RAPIDS Program Office, DEERS Support Office, TRICARE Management Activity-Aurora, and the Joint Uniformed Service Medical Advisory Committee also participate in JUSPAC. The members are the primary people in their organizations responsible for ID card policy execution, benefits and entitlements, DEERS/RAPIDS, and other personnel duties. The Chair of the JUSPAC is rotated among the Army, Navy, Air Force, and Marine Corps. As the CAC is implemented, the JUSPAC should continue its role in policy execution of the Uniformed Services identification card policy execution but also ensure that areas such as civilian personnel identification, DEERS/RAPIDS, and the LRA-RAPIDS integrated workstations are considered in forwarding recommendations on personnel matters. Augmenting the JUSPAC charter to include civilian personnel identification also should be considered.

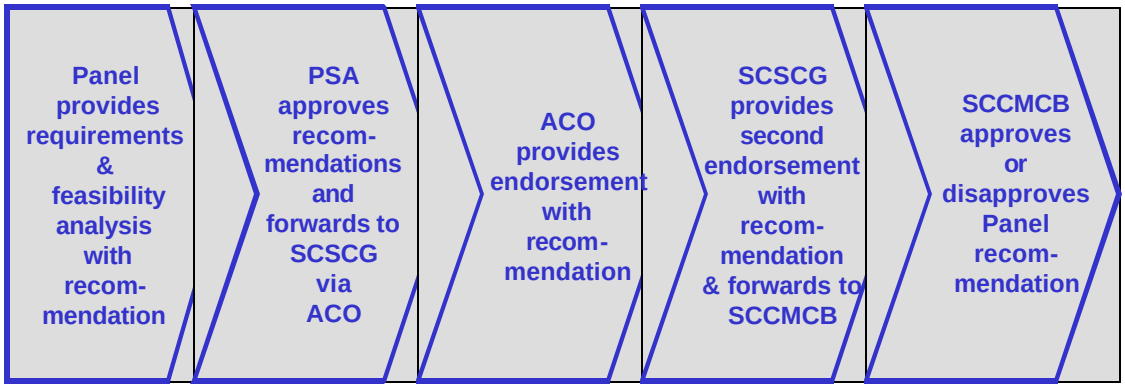
The JUSPAC is a forum through which the Uniformed Services addresses personnel matters (e.g., benefits, entitlements, ID Cards, DEERS, and RAPIDS). Specifically, the JUSPAC will consider the policy implications as the CAC replaces the current Uniformed Services Identification Card. Given the advent of the CAC, the JUSPAC should incorporate the needs of the civilian identification card, physical access, and PKI policy proponents when addressing Uniformed Services Identification Card personnel matters. The JUSPAC will coordinate closely with other Functional Community Panels and Working Groups established to recommend decisions on physical access, PKI, and other future applications approved for Department-wide use.

The JUSPAC also serves as the liaison between DEERS/RAPIDS and the Services. Presently, JUSPAC members review and approve requests for Service-specific DEERS/RAPIDS access, equipment, equipment movement, and other DEERS/RAPIDS program-related issues affecting the Uniformed Services. As the DEERS/RAPIDS infrastructure is aligned to meet the CAC requirements for an integrated LRA-RAPIDS workstation, the JUSPAC's review and approval processes with respect to DEERS/RAPIDS and other DEERS/RAPIDS program areas will be revised to meet the requirements set forth in the LRA-RAPIDS workstation documentation, VO and LRA roles and responsibilities, and PKI policy memoranda.

3.7.6 Approval Process for Department-Wide Applications

The Finance Functional Community Panel and JUSPAC can be used as models for other Functional Community Panels. Figure 12 illustrates a notional approval process to be used by Functional Community Panels to receive approval for Department-wide applications.

Functional Community Panel Department-wide Application Approval Process -- Figure 6



The approval process requires the Functional Community Panel to forward a feasibility analysis with requirements to the SCSCG. The feasibility analysis should include the following:

- Investment and sustainment costs
- Performance enhancements (cost savings, cost avoidance, mission readiness enhancements, quality of life improvements)
- Impact to the Department/Components if not implemented
- Risks associated with implementation
- Migration strategy (impact to operations, infrastructure, technology obsolescence)
- Other alternatives considered.

The Finance Community Panel and JUSPAC establish models for future Functional Community Panels. Other functional areas will benefit from establishing Functional Community Panels to evaluate the feasibility of smart card technology and its impact and/or benefit to their functional area. Functional Community Panels will play a critical role in developing requirements and implementing Department-wide applications using smart card technology. In order to leverage existing DoD and Component infrastructures effectively, it is imperative that functional communities work together to garner value from technology while improving business processes. Further, the SCSCG and SCCMCB will ensure cross-functional integration among Functional Community Panels.

Components should also establish an approval process for Component-specific applications. This process should be approved by the SCSCG.

4. Requirements Planning Methodology

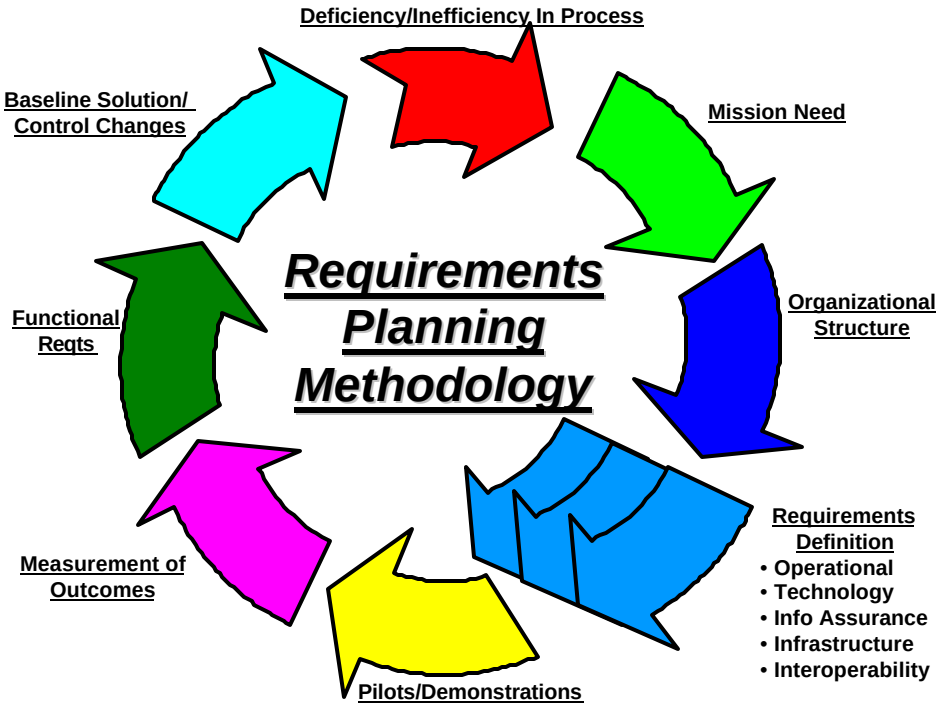
4.1 Introduction

Many mission support areas continue to be inefficient relative to the present day demands and expectations of just-in-time supply, web-based applications and other uses of the Internet, and electronic-based commerce. As an example, Service members still carry folders of paper records with pertinent (sometimes even critical) personnel, pay, medical, and dental information from duty station to duty station. In this era of the Internet, there is a growing deficiency associated with outdated business practices, especially when compared with commercial best practices. Generally speaking, those processes that are paper intensive, have a high volume of transactions, require manual data entry, rely on data security, or are associated with layers of audit, are targets for BPR using smart card technology.

The "Secretary of Defense FY 2000 Report to the President and the Congress" reports that smart card technology is used to facilitate financial management reform by incorporating digital certificates and digital signature capability, creating a paper-free financial transaction with a much higher level of non-repudiation and a more robust audit trail. The Department, its Components, and other federal agencies are embarking on an exciting time of business-based decisions to change the way they operate.

The CAC Requirements Planning Methodology is illustrated in Figure 6. This figure depicts a continuous loop in developing requirements--from identifying a deficiency or need to finalizing a solution. From the deficiency stems a mission need and an organizational structure to support filling the mission need. Next, mission requirements are defined and technical solutions are explored and proposed. Pilots and demonstrations, including advance agreement on metrics appropriate to gauge success, are used to test the feasibility and refine the requirements. The measured outcome of the pilots forms the basis of the functional requirements from which a baseline solution is developed.

Requirements Planning Methodology -- Figure 7



4.1.1 Mission Need

The Department is aware of the need to improve business processes. Using state-of-the-art technology, solutions embedded in the CAC will yield cost savings, improve readiness, enhance mission, support the warfighter, and increase quality of life. In May 1997, a Mission Needs Statement (MNS) for smart card technology was approved and issued. The MNS defined the mission need as the need "to improve the accuracy, timeliness, security, and cost effectiveness of source data and retrieval." The smart card initially was envisioned as an updateable, individually carried, data storage device. Since the approval of the MNS, the mission need has evolved along with technology. That is, the ability to network between computer systems and source data systems has significantly increased, and the smart card has gained capability beyond data storage, such as information processing. With the implementation of PKI, the use of the Internet to transfer data securely and perform online transactions becomes more common and reliable. Electronic business (including electronic commerce/electronic data interchange) has become a mainstay in daily business both in the private and public sectors as a result.

Today, a fully "web-centric" smart card solution is constrained by the current communications infrastructure. For example, connectivity of deployed troops or Sailors underway is sometimes affected by their geographic location or interference, along with operational priorities over communication circuits. Overseas installations are often constrained by antiquated communications infrastructures. The Chip Allocation Technical Work Group has assessed the "web-centric" (on-line) versus "data-centric" (off-line) models and has provided recommendations regarding the CAC Specification.

4.2 Organizational Structure

The Department has evolved its capability to study and support the demonstration of smart card capabilities. The SCTO was formed as outlined in the terms of an August 25, 1997, Memorandum of Agreement (MOA) between the Joint Staff Director for Force Structure, Resources, and Assessment (J8), and the Principal Deputy Under Secretary of Defense (Comptroller). The mission of the SCTO was to conduct an evaluation of smart card technology within the Department to include an on-going demonstration in Hawaii. Within the SCTO charter, the Navy was the designated lead Service to assist and lend expertise to the SCTO. The United States Pacific Command (PACOM) was tasked to manage and execute the smart card technology demonstrations in Hawaii. The SCTO was disestablished in September 1999 consistent with a "sunset clause" in its charter. The ACO concomitantly was established to administer DoD-wide smart card programs as assigned by the DoD CIO and provide support in the execution of smart card policies and programs, including performing central clearinghouse responsibilities for functional and policy requirements.

The DoD ACO will remain the primary organization to monitor requirements planning for the CAC as identified in methodology specified in Figure 6. Deviations will be reported, as appropriate, to the SCSCG and the SCCMCB.

4.3 Generating Requirements

The generation of requirements for the CAC is a multi-faceted process that evaluates the requirements from operational, functional, infrastructure, information assurance, and commercial standpoints. Operational requirements to support the warfighter using the minimum functional requirements (physical and logical access and identification) are being developed in the form of a Joint Operational Requirements Document (ORD). The technical and card topology requirements for the DoD CAC are being further refined using a series of work groups, Functional Community Panels, and the SCSCG. The smart card requirements for a DoD PKI authentication device carrier have been developed

and are awaiting final approval. The OASD(C3I), in coordination with the OUSD(P&R), other Components, and functional communities (e.g. personnel, physical security, and installation management), is developing infrastructure requirements for CAC issuance, certificate management, and maintenance. Finally, government-wide smart card interoperability specifications should be available by the Summer of 2000.

4.3.1 Operational Requirements

As a result of the briefing to the Joint Requirements Oversight Council (JROC) in the Fall of 1999, the Department of the Navy assumed the lead in preparing a smart card ORD for submission to the JROC for final approval no later than July 2000. The ORD for smart card technology will document the requirements needed to support the warfighter and associated combat support missions and functions. The ORD will address the minimum mandatory requirements for the CAC (i.e., authentication, logical access, and physical access). The ORD will stipulate requirements supporting the warfighter in deployed units, training exercises, and daily business functions.

It is the Department's intention that the CAC will be a commercial off-the-shelf (COTS) product. Commercial and industry standards will be used to the fullest extent possible when developing the operational and performance capabilities of the CAC. The minimum mandatory requirements of physical access, logical access, and military and civilian identification/authentication, as well as other approved Department-wide applications, will provide the core requirements identified in the ORD.

The ORD contains Component-specific annexes to identify specific requirements for smart card applications. Approved recommendations from the CAC Chip Allocation and Topology and Policy Recommendation Work Groups that affect operational requirements will be incorporated into the ORD as will those standards generated by the General Services Administration (GSA)-sponsored Government Smart Card Interoperability Specification (GSC-IS) as it relates to physical access, logical access, and identification/authentication using digital certificates. It is important to note that the ORD is a living document established to document current operational requirements. Those results from CAC beta version tests that assist in shaping requirements also will be incorporated into later revisions of the ORD. As mission needs change, requirements or technology may become obsolete, thereby requiring revisions to the ORD. This single ORD will serve as the requirements reference for smart card technology. As technology evolves, the Department intends fully to comply with industry derived standards for smart card technology, similar to computer work stations.

4.3.2 CAC Chip Allocation and Card Topology and Policy Requirements

The core DoD CAC platform will provide physical access to buildings and controlled spaces, logical access to computer networks and systems, and identification for active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractors. Based upon these needs, the SCSCG established two work groups chartered to develop requirements for integrated circuit chip (ICC) allocation and card face topology.

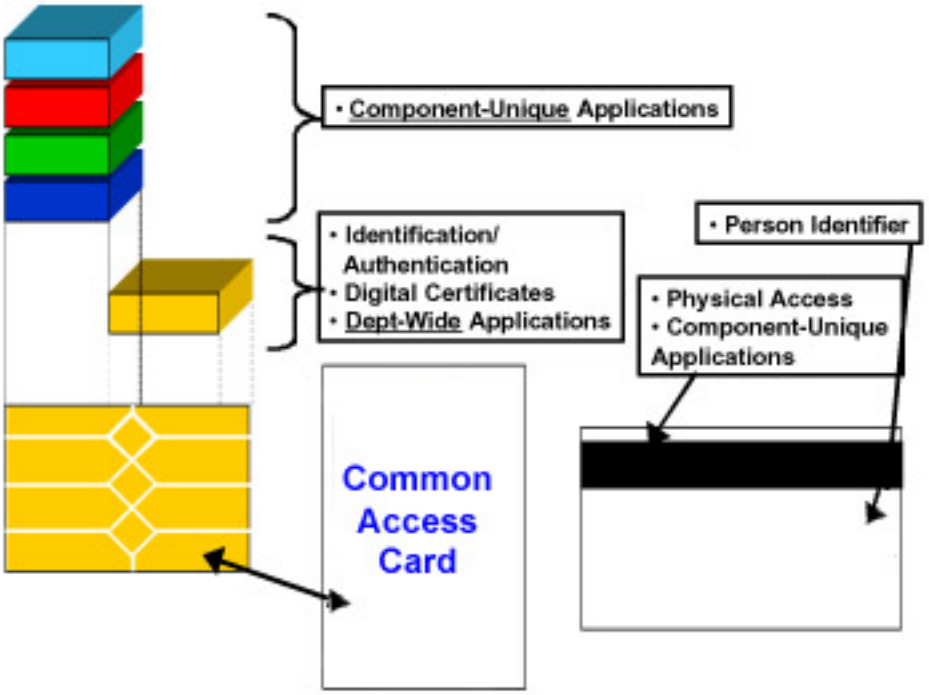
The Chip Allocation Technical Work Group was established by the SCSCG in January 2000. A representative from the Department of the Navy chairs the Group and membership includes personnel from the OSD, Joint Staff, and other Components who have technical backgrounds in smart card architecture. The purpose of the work group is to forward recommendations on the functional and security requirements of the core chip-based functionality, details on the core chip-based functionality, and middleware issues to the SCSCG. The memory and data storage requirements of identification/authentication, logical access, and/or physical access (if migrated to the ICC) functions will affect chip content and allocation. The chip content and allocation will also determine space allocated for supporting multiple applications—Department-wide or Component-specific. In order to define the chip content and allocation, the CAC specific client software (also referred to as middleware) will be determined. It is important to clarify that this work group will not determine Component-specific application requirements. In general, mandated Department-wide applications and those providing warfighter support will take precedence over Component-specific applications in determining memory allocation, but once memory has been allocated to Component-specific applications, it should not be reduced over the life of the CAC. In addition, backward compatibility with Component-specific applications should be maintained over the CAC's lifecycle unless specifically authorized by the SCSCG and SCCMCB. The allocated space or CAC memory for Department-wide and Component-specific applications is provided by this work group and approved by the SCSCG in the form of published CAC Specifications. Based on the evolving nature of smart card technology and lifecycle management considerations, it is expected that this work group will continue to support the SCSCG so long as smart card technology is used by the Department.

The CAC Topology and Policy Recommendation Work Group also was established by the SCSCG in January 2000. This work group is chaired by a representative of the Defense Human Resources Activity (DHRA)--the policy proponent for ID cards (policy support to ACO)--and has members who are policy proponents for the Uniformed Services Identification Cards, civilian identification cards, organizational identification cards, and building physical access cards.

This work group is chartered to provide the SCSCG recommendations on the information to be printed and visible on the card; the functional and security requirements and content of the bar code, magnetic stripe, and two-dimensional (2-D) bar code; and the layout of the card. This work group has concluded its primary tasking and has transitioned to become the CAC Topology and Policy Recommendation Work Group to continue support of the SCSCG in CAC topology and policy areas.

Figure 7 displays a sample of the CAC topology and illustrates how chip allocation and storage will be shared between the CAC and Component-unique applications.

Notional CAC Card Topology & Chip Allocation Considerations -- Figure 8



4.3.3 Hardware Token Technology Requirements

Two efforts are underway to plan and develop requirements for the DoD PKI authentication device carrier (i.e., Class 4 hardware token). These efforts have a direct impact on the CAC since the functionality includes user identity authentication through the use of cryptographic keys.

The first effort, in response to the FY 2000 National Defense Authorization Act, is a report documenting the feasibility of using the smart card as a PKI authentication device carrier. The report concludes that smart card technology is the most feasible solution for authentication to support the DoD PKI.

The second effort, the DoD Target Token Strategy, is a planning document providing a road map for creating a single requirements document for the PKI portion of the CAC platform. The work group charged with developing this strategy document forwarded its draft document to the PKI PMO for review on March 15, 2000.

4.3.4 Infrastructure Requirements

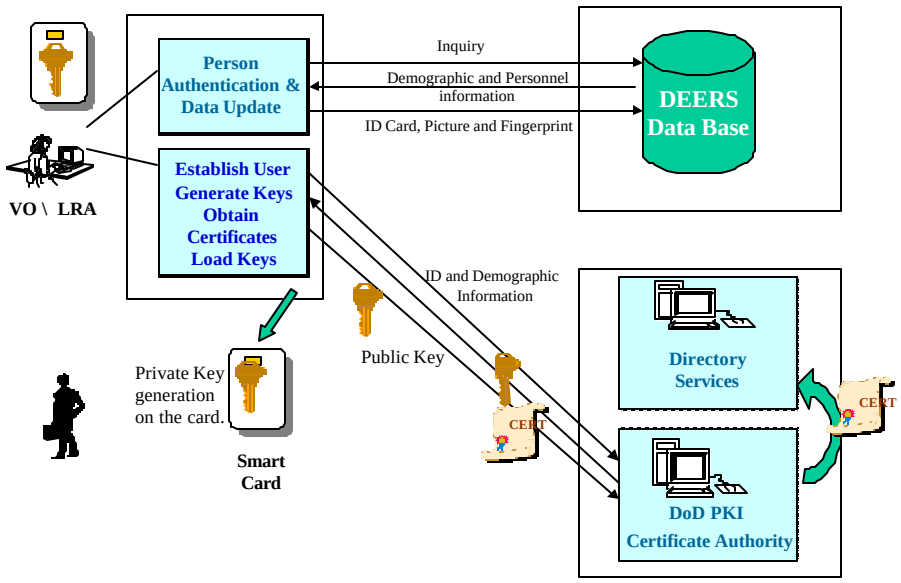
A significant benefit of the CAC implementation is the ability to leverage the existing infrastructure used for issuance of the Uniformed Services Identification Card and smart cards for the CAC. This existing infrastructure includes issuance stations and software applications (via RAPIDS) located throughout the world as well as a comprehensive database (via DEERS) that contains information on Active Duty and Reserve Component (i.e., Guard and Reserve) personnel, DoD civilian employees (with the exception of the Intelligence community), and military family members.

DoD Components and the PKI PMO are working together to take advantage of existing systems and incorporate the necessary security and technical requirements to issue digital certifications and public/private key pairs. The plan to integrate Verifying Official (VO) and Local Registration Authority (LRA) functions into the current issuance station configuration and staffing will allow the issuance of smart cards with identification and authentication (cryptographic keys) capability from the integrated workstations by a single individual. The types of certificate(s) issued by this integrated workstation have yet to be determined but will consist of an identification certificate at a minimum. The program policy covering the VO and LRA functions also will be integrated. For example, the training policy and procedures will incorporate the requirements of the VO and LRA into a single training program.

The integrated workstation is referred to as “LRA-RAPIDS.” LRA-RAPIDS is part of a process that incorporates the functions of the LRA workstation, RAPIDS workstation, and the DEERS database (to include the Card Application Management System), and the Certificate Management System (CMS). The Card Application Management System (CAMS) acts as a security and control feature. Each CAC chip-based application will have a distinctive CAMS. As of the date of this plan, CAMS for the CAC initialization, PKI application. and demographic applet exist. The CMS will support the issuance, maintenance, and revocation of digital certificates. Further details regarding CAMS, CMS, and the

roles, responsibilities, and functions of the LRA-RAPIDS operator and workstation will be provided by a Certification Practice Statement (CPS) and the DoD Common Access Card Issuance Process instruction. A fielding plan, to be completed by August 2000, is being developed to identify deployment milestones for the installation of new LRA-RAPIDS workstations or upgrades of the existing RAPIDS workstations to the LRA-RAPIDS configuration. This fielding plan is in coordination with the CAC rollout schedule. The final integrated LRA-RAPIDS process is illustrated in Figure 8.

LRA-RAPIDS Integrated Process -- Figure 9



In addition to the use of an integrated workstation, a significant benefit of utilizing existing infrastructure is the ability to use trained personnel to maintain the workstations and systems and to staff the workstations during issuance. The VO, using LRA-RAPIDS, will perform LRA responsibilities when issuing the CAC. The VO/LRA must be authorized by the DoD PKI Certification Authority through the CMS and carry an access card with its own authentication certificate. The specific skills and training required for the operator will be detailed in the CPS and the DoD Common Access Card Issuance Process instruction. The objective is to use biometrics as a means to verify the VO/LRA and card recipients' identity to support the security measures of CAC issuance. Biometrics will only be used after full coordination, approval, and regulation at the Department level.

The integrated LRA-RAPIDS is undergoing phased testing and evaluation. The first phase, Pilot I, was developed in coordination with DISA and conducted at the DFAS office at Ford Island (Honolulu, HI) in 1999. The smart card used in this pilot used the magnetic stripe for physical access and a digital certificate loaded on the chip for user authentication. The certificate issuance was performed consecutively on two separate workstations: one for certificate requests and one for certificate downloads. Results from Pilot I were used to improve the LRA-RAPIDS integrated system in Pilot II, which currently is underway. Pilot II is a follow-on technical prototype intended to demonstrate streamlined issuance, increased issuance workstation integration, larger card recipient population, use of key pairs and Department-wide/Component-specific applications together, and prototype the DoD CAC format.

Pilot II began in February 2000 at the DMDC West facility in Monterey, CA and culminated with a demonstration of the integrated workstation at DMDC East for senior DoD leaders on April 25 and 26, 2000. The beta test of a fully functional integrated workstation has been approved and is scheduled for fourth quarter FY 2000. These integrated LRA-RAPIDS tests are being closely coordinated with DISA and the PKI PMO.

4.3.5 Security Requirements

When discussing security and smart card technology, it is helpful to consider the smart card as an individual computer or workstation that is capable of storing data and applications, performing functions on that data, and communicating with other computers, servers, and applications via networks, an Intranet, or the Internet. Using this model, there are two primary areas of concern for overall security: the smart card and associated reader/interface to another system and that other system.

The security of the smart cards being considered for use within the Department is being assessed at many levels (i.e., data and multiple applications on the card, cryptographic services, and biometric services) by multiple agencies. For example, the National Institute of Standards & Technology (NIST) currently is evaluating several smart cards for Federal Information Processing Standard (FIPS) 140-1 compliance. Sandia Laboratories is evaluating the overall security of the integrated circuit chip, and the NSA has performed and is continuing to perform several security assessments of smart card technology. Additional concerns, such as the security of issuance equipment and card stock, are being addressed as part of the integrated work station consideration. Should any CAC security problems or faults arise once the CAC is issued, the SCSCG or a

designated work group will address those issues. The regular meetings of the SCSCG or designated work group will be the conduits by which security problems or faults will be reviewed and resolved. Based upon review by the SCSCG or designated work group, re-issuance or patches to the CAC may occur.

With one exception, the security of the systems with which the CAC will interface is the concern of that system's administrator or cognizant authority. That exception is the integrated VO/LRA workstation, since it closely is tied to the issuance and maintenance off the CAC. The NSA will conduct a separate security assessment on this workstation.

Another area of concern for security is migrating towards a single platform (i.e. the CAC) for physical access within the Department. This area has been addressed within the Department dating back to a 1994 recommendation by the Joint Security Commission. The JSC recommended the development of a uniform badge system for the government's cleared community in a report titled "Redefining Security" that was issued on February 28,1994. In January 1996, the ASD(C3I) supported this concept in a Department-wide memorandum, subject "Uniform Badge System for the Department of Defense." Part of that effort included the work of the Physical Security Equipment Action Group (PSEAG) in establishing the Security Equipment Integration Working Group (SEIWG) specification 012 for the ordering of magnetic stripe information for badging and access control systems. This specification also was made compatible with an earlier pilot by DoD of smart card technology, known as the Multi-Technology Automated Reader Card (MARC). The SEIWG specification has been designated as the standard for all (collateral and Sensitive Compartmented Information (SCI)) DoD badging systems. The CAC will initially support the SEIWG specification via magnetic stripe and will work closely with the DoD physical security community to transition to follow-on technologies, such as contactless smart cards.

4.3.6 Government-wide Smart Card Interoperability Specifications

In January 2000, the GSA issued a Request for Proposal (RFP) to solicit responses from industry to provide the federal government with a common, interoperable, multi-application smart card solution. As part of the contract, the GSA Office of Smart Card Initiatives' Committee for Government Smart Card Interoperability, will form a team comprised both of contractors awarded the Common ID Smart Card contract and government representatives. The team will be responsible for formulating specifications for the Government Common ID Smart Card. The GSC-IS will identify standards for interoperability and testing requirements from multiple commercial sources (e.g., CryptoAPI from Microsoft, JCA/JCE from Sun Microsystems, Common Data Security Architecture (CDSA)

from Intel/OpenGroup and the BioAPI (Version 1) from the BioAPI Consortium). The GSC-IS is scheduled for publication 45 days after contract award. Contract award was announced on May 19, 2000.

The Department has closely participated with GSA in developing an initial draft GSC-IS, a Request for Information (RFI) from industry on smart card technology, and the aforementioned RFP. The Department continues to coordinate efforts with GSA by closely participating in the evaluation of industry team proposals and the selection of the awardees for supplying smart card products and related services to the government. The Department also will participate closely in the development of the GSC-IS. The Department intends to purchase smart card products and services and use the GSC-IS that result from this process to the maximum extent practicable. In doing so, the Department will deploy a CAC that is interoperable with other federal departments and agencies in the key areas of identification, physical access, and logical access. Cryptographic and biometric services will also be interoperable through the GSC-IS. As smart card technology evolves and the Government adopts additional standards and develops specifications, the Department intends to fully comply with and support these technologies to maximize smart card interoperability across the U.S. Government.

4.4 Functional Requirements Definition

The DEPSECDEF memorandum of November 1999 directed the broad functional requirements to be (1) identification of all active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractors; (2) physical access; and (3) logical access (authentication). This direction was defined by available technology as it supported mission need and is based on results from previous business process and technology evaluations and demonstrations. The memorandum defined the minimum mandatory requirements. Knowing that multiple applications result in a higher return on investment, enhanced readiness, and improved quality of life, it is anticipated (and expected) that additional applications will use the CAC platform. The respective Component will develop the functional requirements for its unique applications.

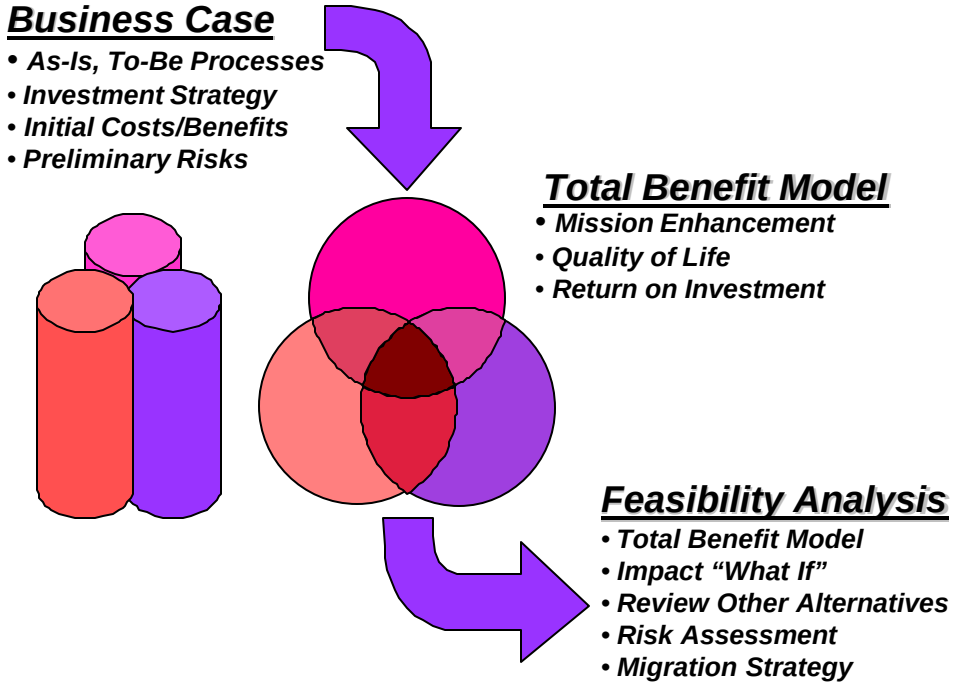
4.5 Exploring Smart Card Technology and Measuring Outcomes

Pilots and demonstrations for smart card technology began in the early 1990s when the DoD Information Technology Policy Board initiated the MARC project to determine if a single card with multiple, updateable technologies could serve the needs of diverse communities within the Department. Initial studies on the

MARC project began in 1993 and continued through 1995. Follow-on smart card pilots and demonstrations continued beyond 1995 to present.

With the establishment of the SCTO in October 1997, several DoD Components began a series of smart card pilots and demonstrations to evaluate the feasibility of employing smart card technology on a DoD-wide basis. The first of a series of these demonstrations using smart card technology were in the Joint Exercise "Cobra Gold 98" and Department-wide applications in Hawaii. Stemming from the Cobra Gold Exercise, a business case analysis (BCA) methodology was developed. The BCA methodology was reviewed and approved by the OSD Director for Program Analysis and Evaluation (PA&E) in April 1998 as a way to measure quantitative and qualitative results from the pilots. Presently, the business case analysis methodology--which features a total benefit model reporting cost savings/cost avoidance, mission enhancement, and quality of life improvements--continues to be the standard for measuring results from the various DoD-wide and Component-sponsored pilots. A business plan documents the business case using the "As-Is" process as a baseline and projecting the costs and benefits of a "To-Be" process. The business plan provides an investment strategy, implementation factors, and risks, if any, for each application or suite of applications. After implementation, a business case analysis documents the actual costs, savings, mission enhancement, and improvements to quality of life. Both the business plan and BCA utilize the total benefit model. That is, they document financial metrics and non-financial factors of the "before" and "after" implementation stages. Figure 9 illustrates the methodology.

Business Case Analysis Methodology -- Figure 10



A total benefit model will be used as part of the feasibility analysis to justify the approval of Department-wide applications on the CAC platform. The Functional Community Panels and Components should use this approach in implementing CAC applications. The total benefit model will include investment and sustainment costs, savings and cost avoidance, mission readiness enhancements, and quality of life improvements. To ensure a consistent and repeatable process, the total benefit model will provide standards for calculating and reporting costs, savings, and intangible benefits such as improvements to mission readiness and quality of life. In addition to the total benefit model, the feasibility analysis will also report on impacts (if not implemented), other alternatives, risks, and a migration strategy. In cases where a Department-wide application is developed as a result of legislatively mandated requirements (e.g., employee or Member privileges or benefits; employee or Member safety), all or portions of the feasibility analysis may not be required.

The measured output from the pilots and demonstrations has been an integral part of the requirements planning methodology for the CAC. Below are criteria that were developed from the pilots and demonstrations to target processes that most benefit from the implementation of smart card technology:

- ?? Paper based/manual or redundant data entry information system
- ?? High number of individual transactions
- ?? Individual records
- ?? Multiple levels of approval, authorization, audit, or review
- ?? Information security requirement
- ?? Physical presence/interaction with customer

The measurement of cost drivers and documentation of qualitative factors have resulted in informed, business-based decisions. On the whole, the results of the pilots have been positive. Lessons learned coupled with total benefit model results have assisted the Department and its Components in building and defining a CAC functionality that optimally supports the mission with acceptable risk.

As the CAC is implemented, a measured output using a total benefit model will be used to evaluate the impact of CAC execution. Appendix B contains recommendations on Performance Evaluation Criteria that may be used to define and determine successful implementation of CAC. Further, lessons learned from previous pilots will be incorporated into CAC execution. Figure 10 identifies general, broad-based lessons learned along with the accompanying solution for CAC execution.

Smart Card Pilots Lessons Learned -- Figure 11

Smart Card Pilots Lessons Learned	Solution for CAC Execution
Evaluate business processes before implementing technology (i.e., don't automate bad processes).	A thorough review of the business processes associated with CAC management, issuance, and logical access (PKI) will be centrally conducted. Physical access processes are site-specific and will require a local evaluation.
Use a systems approach by considering and balancing organizations, processes, and technology.	Apply scientific and engineering efforts throughout the system lifecycle including requirements definition, functional analysis, design, development, testing, integration, installation, and operation.
Yield a higher ROI by using multiple applications on a single platform.	The CAC uses multiple applications on a single platform.
Involve end-users and process owners in requirements development and implementation.	Functional Community Panels and a Communications Plan (i.e., Public Affairs) will involve end-users and functional area proponents.
Communicate benefits and value of new process and technology to cardholders.	A Smart Card Communications Plan (i.e. Public Affairs) is being developed to inform and educate cardholders, benefit providers, functional communities, end-users and decision-makers on features and benefits
Impose configuration management early; ensure that mature applications are readily available.	Configuration management controls and procedures will be detailed in the CAC Configuration Management Plan. A Fielding Plan for Integrated LRA-RAPIDS workstations is in development.
Use a total benefit model to capture both quantitative and qualitative factors – both are required – improvements to quality of life will result in mission enhancement and cost avoidance– need entire picture	A total benefit model will be used to capture cost savings/cost avoidance, mission enhancements, and improvements to quality of life during initial phases of CAC execution.

Ensure interoperability by using industry standards; plan for backward compatibility if there is pre-existing infrastructure.	GSA GSC-IS will be incorporated into CAC implementation. Magnetic stripe and bar code technologies will support backward compatibility of identification and physical access systems. Existing chip applications will be reviewed for inclusion or exclusion on CAC platform.
Assess connectivity and communications bandwidth availability prior to application development and/or smart card enablement.	OUSD (P&R) and OASD(C3I) will develop off-line CAC issuance procedures. Functional Community Panels and Components developing applications will assess connectivity in developing requirements, along with back up procedures to be used in the absence of connectivity.
Assess cards for ease of fraud, duplication, or inherent security risks.	A security assessment will be performed on the CAC along with the integrated issuance stations.
Assess risks associated with immature technology and plan for mitigation.	Target Token Strategy work group will release (proposed) a Request for Information (RFI) to obtain industry feedback on the current COTS capabilities to support and meet DoD Target Token requirements. ORD will document operational performance parameters in concert with industry standards.

4.6 Baseline Requirements and Control Changes

Acceptance tests and procedures for the CAC will be performed by the selected development contractor and managed and approved by the DoD CIO or assigned representative. After testing and upon acceptance by the government, the approved configuration of the CAC will be documented to maintain version control. Configuration management and control procedures will be used to

maintain version control from that point forward. The configuration management procedures (to be detailed in the Configuration Management Plan) specify that an Action Component will be named to assume lifecycle responsibility of each CAC application. An Action Component is an organization responsible for the program management and maintenance of the CAC application. The Action Components for the mandated CAC applications are shown in Figure 11 below.

Department-wide CAC Application Action Component Assignments -- Figure 12

Application	Action Component
Authentication	OUSD(P&R)/DoD CIO
Identification	OUSD(P&R)
Logical Access	DoD CIO/PKI PMO
Physical Access	OASD (C3I)

In addition to configuration management, the Action Component will maintain the application over its lifecycle and will ensure that a problem reporting and troubleshooting process is in place to track user or smart card vendor requests, system problems, and solutions. Changes or modifications to the CAC will be evaluated fully by the Action Component based on technical feasibility, risk, cost, and impact to performance and schedule. The SCSCG and SCCMCB (or designated representative) will review and approve changes or modifications to the CAC baseline platform.

Smart cards still constitute an emerging technology and their application is relatively new to the United States. The technology is gaining ground in the commercial sector for secure authentication and electronic purse functions. As the technology matures, the card industry will continue to develop standards and more robust applications. After initial fielding of the CAC, the Components will likely discover more business processes that will benefit from the use of smart card technology. When that occurs, requirements for the DoD CAC platform will be updated to incorporate technology while still supporting mission needs.

As with any emerging and relatively new technology, the use of smart cards has inherent risk. Additional risks occur in the migration of legacy technologies to the smart card platform. In an effort to mitigate these risks, careful planning and testing must be conducted. Policies must be made for scenarios where the primary means for physical and logical access with the CAC is not available. Each application must have a clear and organized migration plan to successfully implement the CAC.

4.7 Application Development

Support tools, such as developer's kits, web sites/bulletin boards, and developers' conferences will facilitate application development and configuration management at the Department and Component levels. Developer's kits should include test cards, APIs, and documentation. These kits will be issued by the DMDC with each major release of the CAC. The ACO supported web site also will contain a developer's area that facilitates CAC application development with a feedback mechanism for lessons learned, along with a clearinghouse for developed applications. Developers' conferences also will be hosted by the DMDC, as needed, to facilitate development (normally in support of major CAC releases).

4.8 CAC Maintenance

There are two primary concerns regarding CAC maintenance: the lifecycle of the card itself (e.g. bar code(s), magnetic stripe, printed text, hologram, etc.) and the lifecycle of the applications on the card. In order to extend the lifecycle of the card, the text printed on the card (especially that which may change over time) will be minimized and data, functions, and applications will be migrated to the ICC or other updateable media, such as the magnetic stripe. Since the expected lifecycle of the ICC is longer than that of the magnetic stripe, the ICC should be the medium of choice for CAC automated interface. Once migrated to the ICC, the application should be as dynamic as possible, facilitating updates and upgrades without requiring card replacement. Once this capability is established, cardholders may be able to perform updates via their local network, Intranet or the internet vice reporting to DEERS/RAPIDS service centers. The CAC Policy Recommendation Work Group, PKI Working Groups, and CAC Configuration Management Plan are addressing these card maintenance and lifecycle support issues.

5. Configuration Management

5.1 Introduction

The challenges presented in fielding a relatively new technology that will be used by a large, diverse population for multiple applications are significant, but not unmanageable. Establishing a configuration control process early in the development process (prior to deployment) will alleviate potential configuration problems. Components, Functional Community Panels, the ACO, SCSCG, and SCCMCB must work together to ensure that configuration of the CAC platforms and approved applications are maintained and managed.

Initiating change control of the CAC functional requirements specified in the DEPSECDEF memorandum of November 10, 1999, and other approved Department-wide applications is a responsibility of the assigned configuration manager (Component–specific or assigned by the Functional Community Panel for Department-wide applications). Configuration management procedures and policy will be developed centrally by the ACO with recommending and approval authority held respectively by the SCSCG and SCCMCB. An efficient, effective, and flexible configuration management process will be necessary to take advantage of an emerging technology like smart cards. The configuration management process will take into consideration risks imposed by the change and affect the change using the appropriate level of approval authority. Each DoD Component will be responsible for version control of its unique applications.

5.2 Baseline the Smart Card Solution for CAC

The baseline solution for the CAC is defined as a fully functional and tested smart card with identification, authentication/encryption, physical access, and logical access capabilities. The card topology, magnetic stripe, bar code, and chip technology will meet the requirements set forth by the established work groups and approved by the SCSCG and SCCMCB. The baseline solution will include a fully functional infrastructure that is comprised of issuance workstations, database systems, and approved applications--as well as all documentation and training material related to CAC applications and systems. The baseline will be established after beta version testing and security assessment(s). Initial implementation will not occur until the baseline solution is established and documented.

As Components implement the CAC for use with Component-specific systems, such as physical and network access, they will need to conduct further Component and system level testing.

5.3 Technology Direction

The initial version of the CAC will meet the minimum mandatory requirements set forth in the DEPSECDEF memorandum of November 10, 1999, plus additional Department-wide applications that are approved by the SCSCG and SCCMCB. The DMDC is responsible for the technology developments of the CAC platform while Functional Community Panels (for Department-wide applications) or Components (for Component-specific applications) are responsible for CAC applications. Periodically, the DMDC will assess smart card technology to determine if there is potential for obsolescence or proprietary solutions for the CAC. Any negative impact to the current CAC platform will be reported to the SCSCG via the ACO. The DMDC will evaluate how the direction of the technology may fill a previously unmet requirement. Recommendations on how to fulfill that requirement will be forwarded to the SCSCG via the ACO. After each technology assessment, any required changes to the CAC will follow the approved configuration management process found in the Configuration Management Plan. Requirements will be derived from mission need, not new technology. The DMDC also will conduct testing of new applications (Department-wide or Component-specific) prior to fielding to ensure there is no impact on CAC platform performance or security.

5.4 Smart Card Configuration Management Plan

To address the challenges listed above and manage the changes that are evident in a maturing technology, the ACO is preparing a configuration management (CM) Plan. The ACO will provide periodic updates regarding smart cards and related technologies to the SCSCG. The focus for the Department will be to let operational requirements drive technology needs and take advantage of the opportunities that technology affords. The plan addresses how configuration control of the CAC will be managed and maintained at a summary level. The plan also discusses roles and responsibilities of the SCSCG, SCCMCB, Functional Community Panels, work groups, the ACO (as Executive Secretary to the SCSCG and SCCMCB), and the Configuration Managers in CM process.

5.5 Smart Card Configuration Management Control Board

The SCCMCB is comprised of senior level representatives from the Department and its Components. As such, it may not be practical for the SCCMCB to meet regularly to approve all changes to the CAC applications (except during the initial stages of CAC development and implementation). The configuration management process will determine the level at which changes should be made, when to delegate change authority, and how to establish decision-making

thresholds. Criteria will be established to help identify those changes requiring SCCMCB approval and those changes requiring a local review by the Action Component. A layered approach to change control and approval will be used, taking into consideration cost impact, risks to program, and significance of the change. These criteria will be published as part of the CM Plan.

6. Broad Communications

To meet the objective of broad communications, the DoD ACO is developing a web site to publish CAC progress, smart card technology updates, results from pilots and demonstrations, and Functional Community Panel activities. The web site will provide a central communication clearinghouse to document progress. The functional process owners will be able to access the web site to monitor the status of the Functional Community Panels' recommendations regarding the use of smart card technology. Functional Community Panel points of contact also will be published so members of a functional community can contact their Component's representative regarding specific issues. This web site is continually updated and revised; a beta version was fielded in July 2000. Updates to the web site will be posted as improvements and relevant data sources are identified.

Another action to enhance broad communication for the entire CAC population is the development of the CAC Communications Plan. This plan will outline a strategy for informing and educating CAC end-users to include cardholders and benefit providers, Functional Community Panel members, decision makers (e.g., PSAs, SCSCG and SCCMCB members), and others on the CAC purpose, operation, benefits, and value. This campaign is critical to the overall success of the CAC, and the Communication Plan will serve as a roadmap to ensure that all parties are informed and adequately trained on the CAC features and benefits. A final CAC Communications Plan was issued in July 2000.

The development of the Communications Plan and the web site to publish up-to-date progress and results will assist the ACO in its role of serving as a clearinghouse for information and ideas between and among functional communities. The CAC Communications Plan addresses cardholders, the type of information each user community will require, and how the information will be delivered. This plan will be reviewed and approved by the Office of the Assistant Secretary of Defense (Public Affairs).

The Communication Plan will detail the delivery of targeted information for various user communities. The CAC policy makers (i.e. SCSCG chair and members, SCCMCB chair and members, smart card program managers, and Functional Community Panel members) will receive an internal marketing campaign that will be delivered using leadership and subject matter experts as internal communicators along with materials such that all entities provide a consistent message. Senior leadership in DoD and federal government, including agency directors, federal managers, Service secretaries, agency directors, CIOs, flag/general officers, and commanding officers will be provided

CAC information at an overview (high) level, including the benefits of CAC to the Department, its Components, and other federal agencies. This information can include cost savings, infrastructure leverage, mission enhancement, and quality of life and will be delivered by media such as video and the CAC web site. Others, such as technology managers and deputy CIOs, will require more detailed briefing materials on the specifics of smart card technology (e.g. ICC, bar code, and magnetic stripe).

The Communication Plan will need to provide CAC physical and logical access information, such as how it works, results of security assessments, impact to physical security and computer LAN/WAN administration policy and procedures to physical security managers/military & base police and information assurance/ system administrators, respectively. The VO/LRA and DEERS/RAPIDS operators also will need detailed information, such as impacts and changes to the overall process for issuing smart cards, provided through formal training and documentation. Process owners will need to know business process changes and policy changes (resources, staffing). Commanding officers should be aware of CAC benefits, such as command security, information security, cost savings, impacts to base and commands (e.g. disruptions), and implementation schedules.

Another consideration of the Communication Plan will be the global user community. Users need to become aware of the CAC, how to obtain cards (issuance procedures), similarities to and differences between it and the previous identification cards, software tokens, and physical access badges, changes that they can expect, and how this *helps them* do their job better, faster, and/or cheaper. Finally, private sector vendors and the public should be informed regarding the CAC's potential impact on commerce and business practices, its similarities or differences to the military ID card, and the possibility that civilians may carry the cards as well.

7. Summary

The CAC will result in re-engineered business processes, enhanced mission readiness, improved information security, and improved quality of life to the members of the Department and its Components. As this Execution Plan documents, there is an aggressive schedule planned for the next year. As with all programs, execution does not come without risks. Consequently, key personnel are meeting daily to address and mitigate these risks to an acceptable and executable level. Figure 13 lists known schedule and technical risks directly impacting the CAC program.

CAC Program Risks and Mitigation -- Figure 13

Risk Area	Mitigation
Schedule Significant decision milestones will need to be made in the next 60 days including: ?? PKI Requirements ?? Use of Floppy Diskettes for Class 3 Tokens ?? Definition of Class 4 Token	Meet schedule milestones as documented in CAC Execution Plan and other planning documents. Expedite and accelerate decisions when necessary (i.e., long-term impact if near term milestones are not met).
Material ?? Availability of silicon for ICC ?? Potential for shortage of silicon due to foreign and commercial demand on smart cards in the next 12 months	Meet requirements definition schedule dates to reach smart card decision in a timely fashion. Continue discussions with industry analysts to monitor potential shortage. Plan for procurement in advance of projected demand.
Costs ?? Cost per smart card must remain close to $6 projection to meet budget ?? Decision on smart cards based on requirements may impact unit cost	Meet requirements definition schedule dates, identify cost impact as part of the FEA, incorporate FEA results or other cost deviations into POM02 submission.
Backward Compatibility Ensure CAC meets existing smart card users' operational requirements and infrastructure	CAC platform specifications will address backward compatibility with smart cards already issued to Service Members and DoD civilians. Fielded CAC will meet CAC platform specifications. The existing DoD systems: Defense Travel System, Wide Area

Risk Area	Mitigation
	Work Flow, and Electronic Document Access have made changes to accept digital certificates using smart card as the hardware token.
CAC Security ? ? Identity Theft ? ? Reciprocity ? ? Database/LAN/Intranet Access ? ? CAC turn-in/exchange for visitor access	Conduct analyses and studies; address in work groups and Functional Community Panels; support with policy promulgation.
PKI Related Issues ?? Communications availability ?? Certificate expirations coinciding with Identification expirations (potential for spikes in issuance) ?? Physical security requirements of CAC and LRA-RAPIDS workstations ?? Personnel requirements of LRA-RAPIDS workstations	The ACO, DMDC, NSA and PKI PMO presently are addressing all of these issues. Specifically, an implementation strategy for the integrated LRA-RAPIDS workstation will address how the workstations will be deployed. Other discussion items are workstation physical security, VO/LRA training requirements, the use of S/W certificates in the near term, directory integration, policy resolution.

7.1 Budget

The Department has budgeted $13.1 million for FY 2000 and $31.9 million for FY 2001. An ongoing Front End Assessment (FEA) for the program objective memorandum (POM) 2002 process will address remaining budget requirements for FY 2002 throughout the future years defense plan (FYDP).

This budget includes four major categories: cards, RAPIDS infrastructure upgrades, DEERS/RAPIDS, and ACO operations. The cards category includes card stock, consumables, and card distribution. The RAPIDS Infrastructure Upgrades include funding for hardware and software, installation and maintenance, and training. The DEERS/RAPIDS category includes DEERS hardware/ software funding along with DEERS/RAPIDS smart card software development. The ACO funding includes program management support for the CAC. These items are listed in Figure 14.

CAC Budget in FY 2000 $, rounded to the nearest $1,000 -- Figure 14

Budget Item	FY2000	FY2001
Cards	855,000	9,536,000
RAPIDS Infrastructure Upgrades	1,994,000	9,826,000
DEERS/RAPIDS	8,648,000	10,048,000
ACO	1,551,000	1,468,000
TOTAL	13,048,000	30,878,000

7.2. Conclusion

The DoD organization, requirements, resources, and schedule are in place to ensure that the CAC is executed on time and consistent with stated requirements. Components may require additional time to plan, develop requirements, and budget for CAC use. Critical near-term decision milestones have been addressed in order to finalize the CAC platform specifications which, in turn, will decide the initial smart card type, chip allocations, and card topology. The schedule to begin implementation by October 2000 is aggressive but can be executed with continued cooperation from the key organizations within the Department and its Components as well as the Functional Community Panels and other infrastructure. Appropriate communications and meetings of the SCSCG and the SCCMCB are critical to the top-down management attention and CAC success. Successful execution of the CAC will be a significant part of the Department's continued commitment to innovative use of BPR and technology to improve business practices.

Appendix A - List of Acronyms

Abbreviation of Term	Explanation
ACO	Access Card Office
AGR	Active Guard and Reserve
ASD	Assistant Secretary of Defense
ATSD	Assistant to the Secretary of Defense
CAC	Common Access Card
CAMS	Card Application Management Systems
CDSA	Common Data Security Architecture
CINC	Commander-In-Chief
CIO	Chief Information Officer
CMS	Certificate Management System
COTS	Commercial Off-The-Shelf
CPS	Certificate Practice Statement
DDR&E	Director of Defense Research and Engineering
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DFAS	Defense Finance and Accounting Service
DHRA	Defense Human Resources Activity
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DON	Department of Navy
DOT&E	Director of Operational Test and Evaluation
FEA	Front End Assessment
FIPS	Federal Information Processing Standard
FY	Fiscal Year
GIG	Global Information Grid
GSA	General Services Administration
GSC-IS	Government Smart Card Interoperability Specification
IC	Intelligence Community
IG	Inspector General
IMA	Individual Mobilization Augmentees
ING	Inactive National Guard
IRR	Individual Ready Reserve
ITSCC	Information Technology Standards Coordinating Committee

Appendix A - List of Acronyms (cont'd)

Abbreviation of Term	Explanation
JROC	Joint Requirements Oversight Council
JSC	Joint Security Commission
JUSPAC	Joint Uniformed Services Personnel Advisory Committee
JTA	Joint Technical Architecture
LRA	Local Registration Authority
MARC	Multi-technology Automates Reader Card
MNS	Mission Needs Statement
MOA	Memorandum of Agreement
NAVSUP	Naval Supply Systems Command
NIST	National Institute of Standard and Technology
NMCI	Navy and Marine Corps Intranet
NSA	National Security Agency
OASD	Office of Assistant Secretary of Defense
OUSD	Office of the Under Secretary of Defense
OGC	Office of General Counsel (DoD)
ORD	Operational Requirements Document
OSD	Office of Secretary of Defense
OUSD	Office of Under Secretary of Defense
PACOM	United States Pacific Command
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKI PMO	Public Key Infrastructure Program Management Office
PSA	Principal Staff Assistant
PSEAG	Physical Security Equipment Action Group
RAPIDS	Real-Time Automated Personnel Identification System
RFI	Request for Information
RFP	Request for Proposal
ROI	Return on Investment
SBU	Sensitive But Unclassified
SCCMCB	Smart Card Configuration Management Control Board
SCI	Sensitive Compartmented Information
SCO	Smart Card Office
SCSCG	Smart Card Senior Coordinating Group
SCTO	Smart Card Technology Office
SEIWG	Security Equipment Integration Working Group
SES	Senior Executive Service

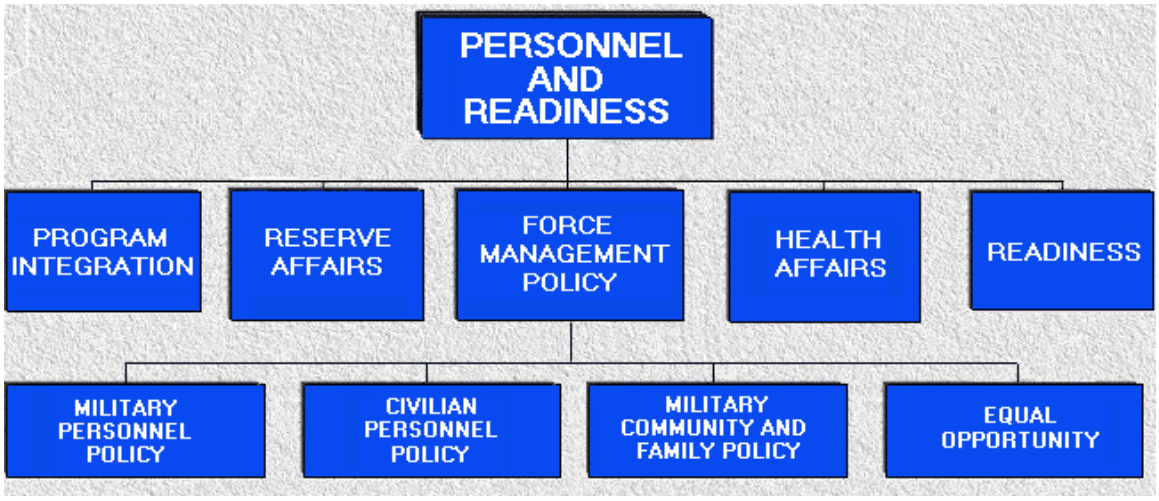
Appendix A - List of Acronyms (cont'd)

Abbreviation of Term	Explanation
SSN	Social Security Number
USD	Under Secretary of Defense
VO	Verifying Official

Appendix B - Performance Evaluation Criteria

Measurement Area	Measures of Success
Program Schedule	? ? Meet timeline directed by DEPSECDEF 10 Nov 99 memorandum to deploy the DoD CAC to multiple locations by December 2000 ? ? CAC infrastructure in place by September 30, 2001
Interoperability	? ? SCSCG integration of Smart Card requirements with Military Departments and Agencies and the PKI PMO ? ? Integration goal provides fully interoperable, backwards compatible, and commercially derived solution capable of working with planned or legacy systems ? ? CAC specifications in concert with GSA Government Smart Card Interoperability Specification
Readiness	? ? Number of indirect hours converted to direct support hours ? ? Reduction in time required to prepare for deployment
Quality of Life	? ? Improvement of customer service functions ? ? Elimination of redundant paperwork ? ? Reductions in transportation time
Mission Enhancement	? ? Elimination of unnecessary administrative tasks ? ? Overall improvement of data quality ? ? Streamlining or elimination of audit functions
Re-engineering	? ? Use of business case analysis methodology to calculate return on investment and document other non-financial metrics
Use of Existing Infrastructure	? ? Use existing infrastructure to gain efficiencies ? ? Physical access, LRA and ID costs compared with integrated work station
Information Assurance	? ? Did smart card technology improve information assurance
Cardholder Audience	? ? Reach the targeted population within timeframe ? ? Targeted population made aware of CAC functions, value and benfits

Appendix C – OUSD(P&R) Representation



Appendix D – Bibliography of CAC Execution Related Documents

1. DEPSECDEF Memorandum, “Smart Card Implementation and Adoption”, 10 November 1999
2. Configuration Management Plan For the Common Access Card (Draft)
3. Fiscal Year 2000 Defense Authorization Act (Public Law 106-65) of October 1999
4. Department of Defense Charter, “Smart Card Configuration Management Control Board”, 14 April 2000
5. Department of Defense Charter, “Smart Card Senior Coordinating Group”, 14 April 2000
6. DoD Access Card Office Charter, 27 April 2000
7. Department of Navy (DON) Smart Card Office (SCO) Re-engineering Phase I Business Plan for Personnel Support Detachment Pearl Harbor (June 1999)
8. Department of Defense Certificate Policy (Draft)
9. Department of Defense (DOD) RAPIDS LRA Certification Practice Statement (CPS) (Draft)
10. Government Smart Card Interoperability Specifications (GSC-IS) (Draft)
11. Secretary of Defense FY 2000 Report to the President and the Congress
12. Mission Needs Statement (MNS) for smart card technology, May 1997
13. Operational Requirements Document (ORD) For The Joint Smart Card (Draft)
14. Common Access Card Release 1.0 ICC Requirements (Draft)
15. Consideration of Smart Cards as the DoD PKI Authentication Device Carrier, 10 January 2000
16. DoD Target Token Strategy (Draft)
17. DoD Common Access Card Issuance Process (Draft)
18. Security Equipment Integration Working Group (SEIWG) specification 012
19. Smart Card in Cobra Gold ’98 Business Case Analysis, January 1999
20. CAC Communications Plan (July 2000)
21. CAC Fielding Plan (Draft)
22. CAC Front End Assessment